

Fig. 1

Version	1.1
Serial Number	12345
Signature Algorithm	RSA+MD2, 1024
Issuer	C=US, S=NY, O=Xcorp
Validity	1/1/98 - 12/31/99
Subject	C=US,S=NY, O=Xcorp,CN=John
Subject Public Key Info	RSA, 1024, public key value
Other info.	Roles, policies, reliance limits, etc
Signature of CA	(based on all the above, public info and CA's private key

Fig. 2

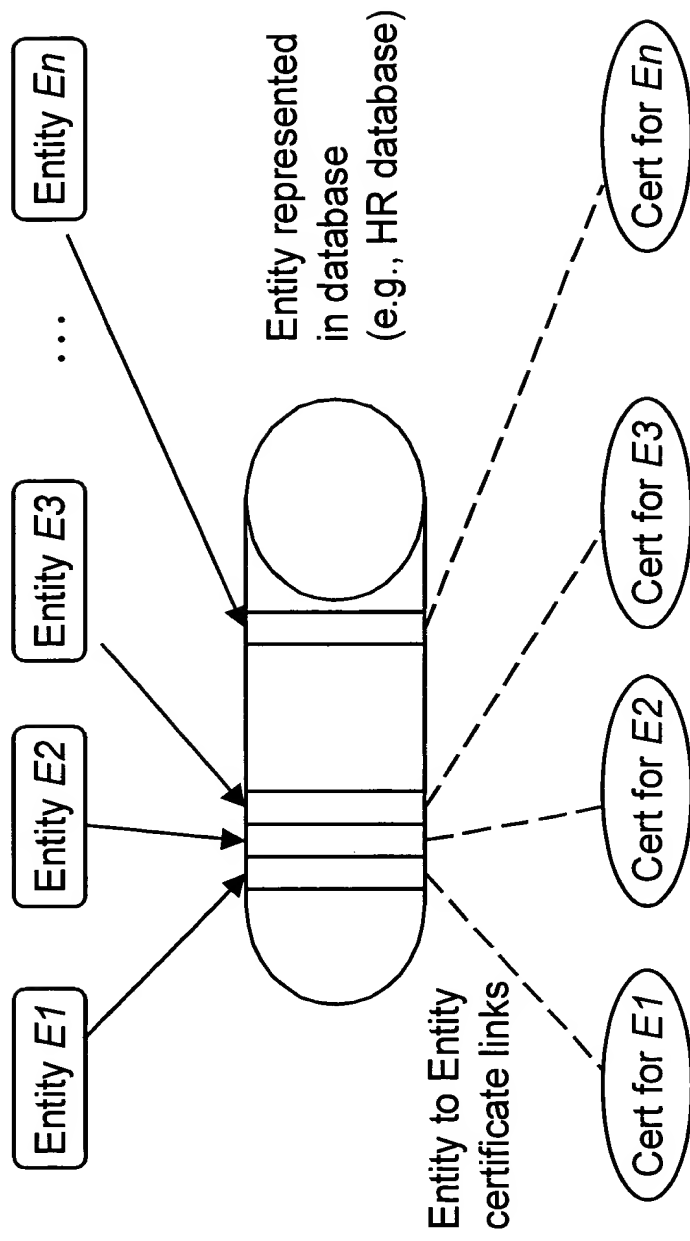


Fig. 3

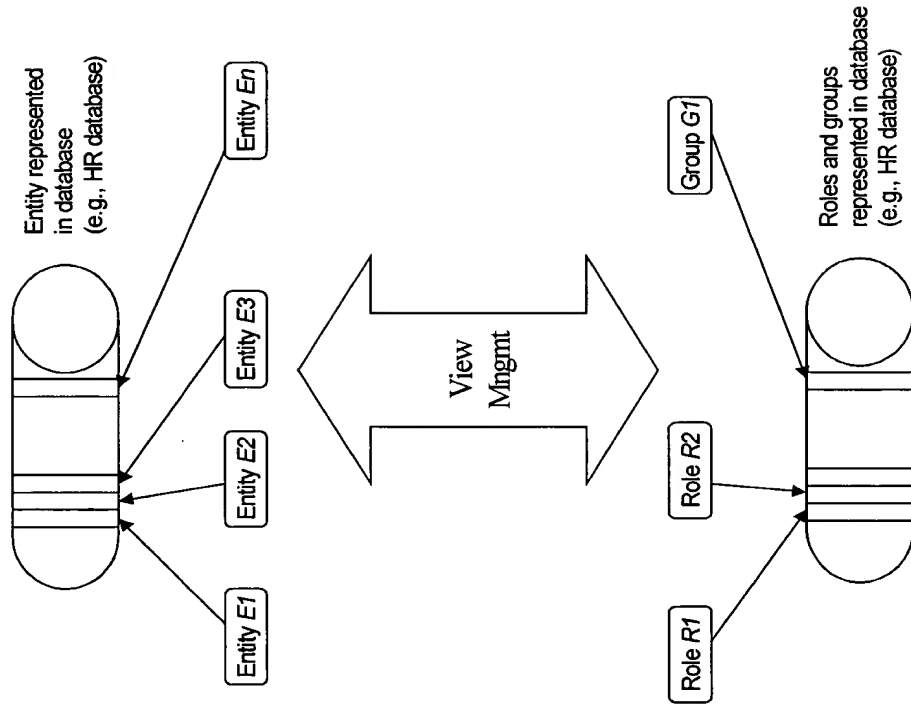


Fig. 4

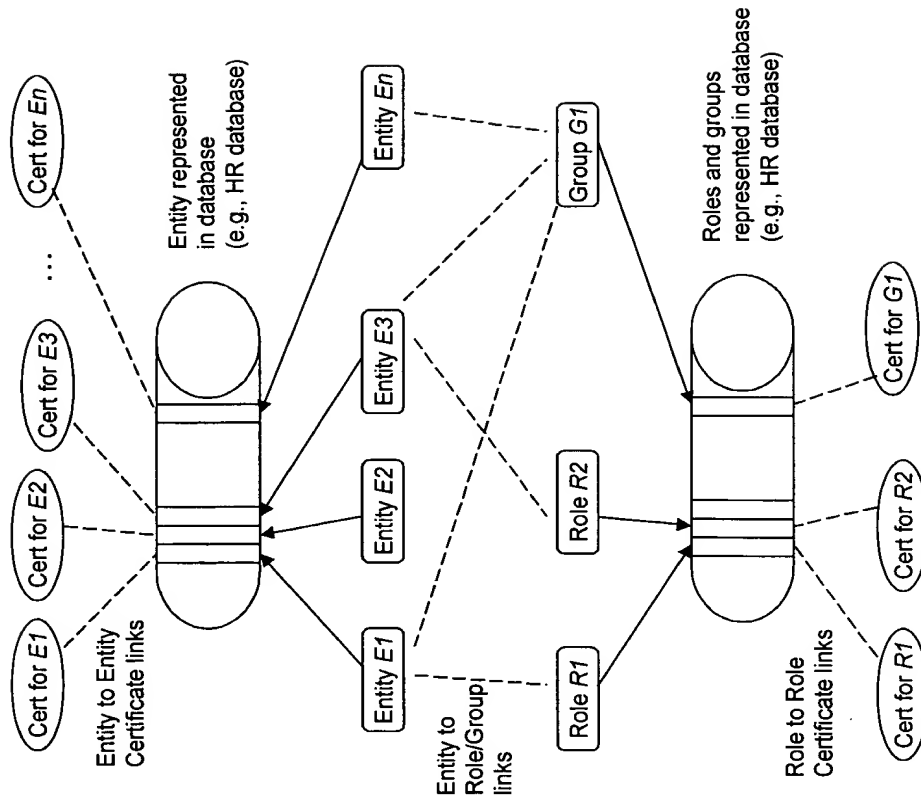
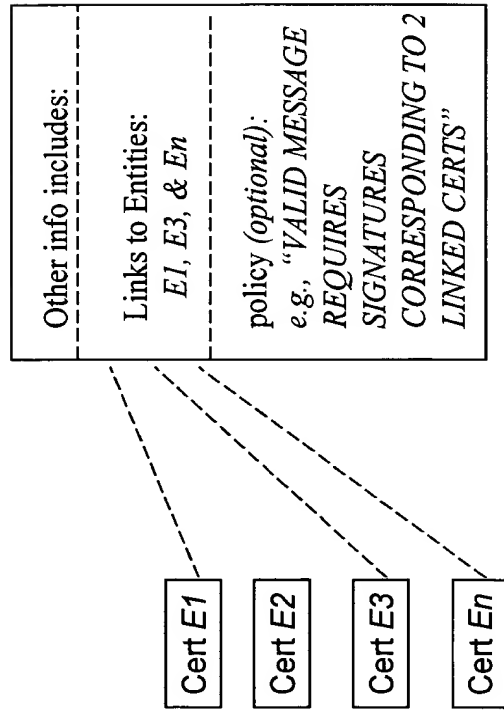


Fig. 5

Explicit group *G1* certificate



Valid message from *G1*

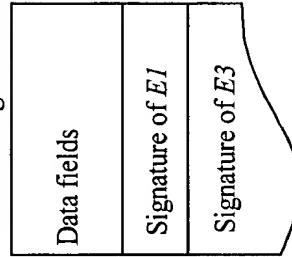
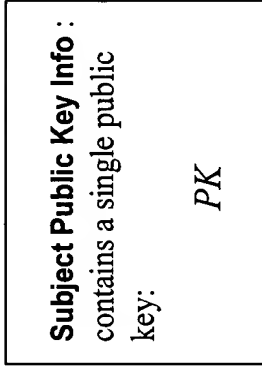


Fig. 6

Implicit group certificate



Valid message from group

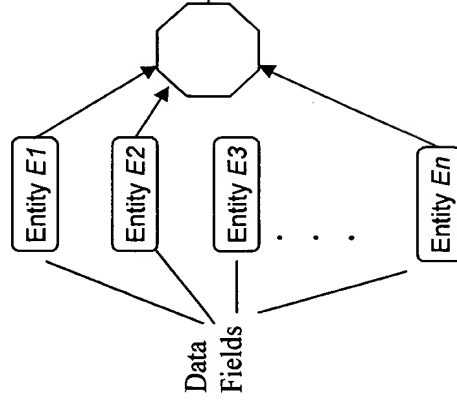
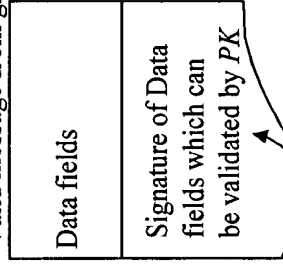


Fig. 7